REMARKS

In response to the Official Action of October 3, 2006, claims 1, 2, 9, 10, 15, 17-19, 25 and 26 have been amended.

In particular, claim 18 has been amended to overcome the rejection of this claim under 35 USC §112, second paragraph. At page 2 of the Official Action, it is stated that claim 18 is indefinite because the specification does not provide an adequate disclosure showing what is meant by "processing mean (127) for outputting". The quoted portion of claim 18 has been amended to recite "a processor configured for outputting the unique chip identifier". Support for this amendment to claim 18 is found in the specification as originally filed, including page 9, lines 9-23. Claim 18 is therefore believed to be definite.

Referring now to the rejection of claim 1 under 35 USC §103, it is noted at page 3 that claim 1 and claims 3, 4, 6, 8, 9, 11, 12, 14, 16, 18, 20, 21, 23, 24 and 25 are rejected under 35 USC §103(a) as being unpatentable over US patent application publication 2002/0147920, Mauro, in combination with US patent application publication 2002/0150243, Craft et al (hereinafter Craft).

It is asserted that Mauro discloses a method for managing cryptographic keys that are specific to a personal device with the method being performed by a secure processing unit arranged in communication with the personal device and reciting the actions set forth in claim 1 except that it is asserted that Mauro does not disclose other features of claim 1, such as receiving in response to storing the data package, associating the unique chip identifier with the received backup data package and storing the backup data package in the associated unique chip identifier.

The Office further asserts at page 4 of the Official Action that Craft discloses the other features as set forth in claim 1, such as receiving, in response to storing the data package, a backup data package from the device, which backup data package is the data

package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the chip.

Applicant respectfully disagrees. As seen in Figures 1 and 2 of Mauro, it discloses a remote terminal (110) which includes a system memory (236), a main processor (230), and a secure unit (240) as described at paragraphs 31 and 32. The main processor (230) is disclosed as vulnerable to attack from external input/output lines, as well as from over-the-air negotiation (see paragraph 33). Therefore, Mauro teaches that the secure unit (240) performs all secure processing and stores all "sensitive" data, which sensitive data includes any data desired to be prevented from unauthorized access (see paragraph 34). Figure 2 of Mauro is a diagram of a specific embodiment of the secure unit (240) (see paragraphs 35-40).

Claim 1, as amended, specifically is directed to a method for managing cryptographic keys that are specific to a personal device and comprises retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device. As seen in Figure 3 of Mauro, the secure unit (240) is within a remote terminal. This is specifically pointed out at paragraph 18 of Mauro which describes Figure 3 as a diagram of a specific embodiment of the secure unit within the remote terminal. Consequently, the retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from the personal device is not possible in Mauro since the secure unit is part of the personal device.

Furthermore, the action recited in claim 1 of retrieving in a secure processing point a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device is not shown in Mauro. Rather, Mauro shows in Figure 3 that a read-only memory (ROM) (252) which is implemented within the secure processor (250) forming part of the secure unit (240) actually performs the securing of parameters which become available for use thereafter as explained at paragraph 38.

Claim 1 further recites storing a data package in the device, the data package including at least one cryptographic key. This storing operation is performed by the secure processing device with respect to the personal device and thus there is communication from the secure processing point to the personal device. The data package is stored in the personal device which is a physical entity different from the secure processing point.

In Mauro, it is shown that sensitive data is stored in secure unit (240) itself or in system memory (236) (see Figure 3) and therefore the secure unit and the sensitive data are, according to Mauro, included in one and the same physical entity that is in the form of the remote terminal. This is in contradistinction to the requirement of claim 1 wherein the secure processing point stores a data package in the personal device, the data package including at least one cryptographic key.

With regard to the other requirements of claim 1, the Office asserts that Craft makes up for the deficiencies in Mauro. Applicant respectfully disagrees. In particular, Craft is directed to a method and system for controlled distribution of application code and content data within a computer network. It is shown in Craft that a client device is configured to download application code and/or content data from a server operated by a service provider. Embedded within the client is a client private key, a client serial number, and a copy of a server public key. The client forms a request, which includes the client serial number, encrypts the request with the server public key and sends the download request to the server. The server in turn decrypts the request with the server's private key and authenticates the client. The received client serial number is used to search for a client public key that corresponds to the embedded client private key (see Craft abstract).

The Office asserts that Craft suggests receiving, in response to storing the data package, a backup data package from the device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the chip. Claim 1, as amended, requires that this receiving is at the secure

processing point. Instead, Craft shows retaining and storing the client serial number and client public key in a public key datastore (see paragraph 43). Retaining and storing a client serial number and client public key in a public key datastore is completely different from receiving a data package encrypted with a secret key of the chip. Thus, even if, for purposes of argument, Mauro and Craft could be combined as argued by the Office, such a combination would not suggest the present invention as it fails to teach most of the requirements of claim 1 as enumerated above.

It is therefore respectfully submitted that claim 1, as amended, is distinguished over Mauro in view of Craft. Since claim 1 is believed to be distinguished over Mauro in view of Craft, it is respectfully submitted that claims 3, 4 and 6, all of which ultimately depend from amended claim 1, are further distinguished over the cited art.

Furthermore, independent system claim 9, independent personal device claim 18, and independent secure processing point claim 25 are also distinguished over Mauro in view of Craft for similar reasons as those presented above with respect to claim 1.

It is therefore further submitted that claims 11, 12 and 16, which ultimately depend from amended independent claim 9, and claims 20, 21, 23 and 24, which ultimately depend from amended independent claim 18, are further distinguished over the cited art.

It is further submitted that dependent claims 2, 5, 10, 13 and 22 are distinguished over Mauro and Craft as applied to claims 1, 9 and 18, further in view of US patent application publication 2002/0157002, Messerges et al, since each of these claims ultimately depend from an amended independent claim which is believed to be distinguished over the cited art.

Similarly, the rejection of claims 7, 15 and 26 as unpatentable over Mauro and Craft as applied to claims 1, 9 and 25, further in view of US patent 5,892,900, Ginter et al, is believed to be overcome since each of these claims ultimately depend from an amended independent claim which is believed to be distinguished over the cited art.

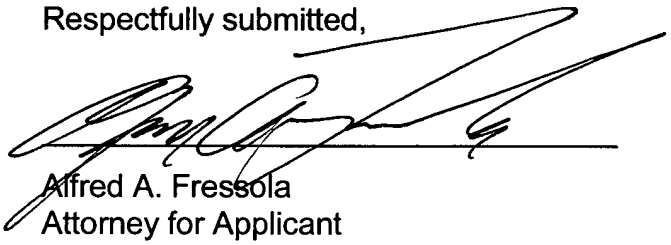
Independent method claim 17 is rejected under 35 USC §103(a) as unpatentable over Mauro and Craft as applied to claim 1, further in view of US patent 5,564,032, Aota et al. This claim is believed to be distinguished over the cited art due to its dependency from amended claim 1.

Finally, dependent personal device claim 19 is not suggested by Mauro and Craft further in view of US patent 6,654,465, Ober et al, due to its dependency from amended claim 18 which is distinguished over the cited art.

In view of the foregoing, it is respectfully submitted that the present application as amended is in condition for allowance and such action is earnestly solicited.

The undersigned respectfully submits that no fee is due for filing this Amendment. The Commissioner is hereby authorized to charge to deposit account 23-0442 any fee deficiency required to submit this paper.

Respectfully submitted,



Dated: January 2, 2007

Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955